

# On the Computation of the Galois Group of Linear Difference Equations

Ruyong Feng\*

KLMM, AMSS, Chinese Academy of Sciences,  
Beijing 100190, China

## Abstract

We present an algorithm that determines the Galois group of linear difference equations with rational function coefficients.

## 1 Introduction

The current algorithms for computing the Galois group of linear difference equations were only valid for the equations of special types, such as the second order equations, the equations of diagonal form or with constant coefficients and so on. In [9], a difference analogue of Kovacic's algorithm was developed for linear difference equations of order two. In [23], algorithms for linear difference equations of diagonal form were developed. For linear difference equations with constant coefficients, an algorithm can be found in [22], where the author further showed that there is a recursive procedure that derives the Galois group from the ideal of algebraic relations among solutions, and vice versa. In [15], Maier gave upper and lower bounds for the Galois groups of Frobenius difference equations over  $(\mathbb{F}_q(s, t), \phi_q)$ , where  $\phi_q(s) = s^q$  and  $\phi_q(a) = a$  for all  $a \in \mathbb{F}_q(t)$ . On the contrary, algorithms for computing the Galois groups of linear differential equations have been well-developed (see [2, 13, 20, 11]). Particularly, in [11], Hrushovski developed an algorithm that calculates the Galois groups of all linear differential equations with rational function coefficients. His algorithm involved many arguments from logical language and has recently been reworked by Rettstadt in [17] and by the author in [7]. Here, in this paper, we develop an algorithm for computing the Galois group of linear difference equations with rational function coefficients of arbitrary order. Our algorithm can be considered as a difference analogue of Hrushovski's algorithm.

The philosophy of computing the Galois groups of linear difference equations is quite similar to that of linear differential equations. The Galois groups of these two kinds of equations are linear algebraic groups over the field of constants. Hence bounds for the defining equations of linear algebraic groups developed for the differential case can be applied to the difference case without any modification. However, there exist some results in differential algebra whose difference analogues are not correct any more, and vice versa. For example,

---

\*ryfeng@amss.ac.cn. This work is partially supported by a National Key Basic Research Project of China (2011CB302400) and by a grant from NSFC (60821002).

associated primes of a radical differential ideal are again differential ideals, while those of a radical  $\sigma$ -ideal need not be  $\sigma$ -ideals but  $\sigma^\delta$ -ideals for some integer  $\delta$ . This forces us to consider  $\sigma^\delta$ -ideals. Another example is that the Picard-Vessiot extension ring for linear differential equations is not necessarily the coordinate ring of a trivial torsor for the Galois group, while that for linear difference equations is the coordinate ring of a trivial torsor. This implies that one only needs to consider objects such as hypergeometric elements that are defined over the basic field.

Throughout this paper,  $k$  stands for the field of rational functions in  $x$  with coefficients in  $\overline{\mathbb{Q}}$ , the algebraic closure of the field of rational numbers, and  $\bar{k}$  stands for its algebraic closure. The difference field which we are interested in is the field  $k$  with an automorphism  $\sigma$  given by  $\sigma(x) = x + 1$  and  $\sigma(c) = c$  for  $c \in \overline{\mathbb{Q}}$ . Consider the following linear difference equations

$$\sigma(Y) = AY \tag{1}$$

where  $Y$  is an  $n \times 1$  vector with indeterminate entries and  $A \in \text{GL}_n(k)$ . Let  $R$  be the Picard-Vessiot extension ring of  $k$  for (1). The Galois group of (1) over  $k$ , denoted by  $\text{Gal}(R/k)$ , is defined to be the set of  $\sigma$ - $k$ -automorphisms of  $R$ , i.e.  $k$ -automorphisms of  $R$  that commute with  $\sigma$ . Let  $F$  be a fundamental matrix of (1) with entries in  $R$ , i.e.  $F \in \text{GL}_n(R)$  satisfying  $\sigma(F) = AF$ . Then for any  $\phi \in \text{Gal}(R/k)$ ,  $\phi(F)$  is another fundamental matrix of (1). Thus there exists  $[\phi] \in \text{GL}_n(\overline{\mathbb{Q}})$  such that  $\phi(F) = F[\phi]$ . The map given by  $\phi \rightarrow [\phi]$  is a group homomorphism of  $\text{Gal}(R/k)$  into  $\text{GL}_n(\overline{\mathbb{Q}})$ . Denote by  $G$  the set  $\{[\phi] \mid \phi \in \text{Gal}(R/k)\}$ . It was proved in (Theorem 1.13, page 11 of [23]) that  $G$  is a linear algebraic group defined over  $\overline{\mathbb{Q}}$ . The reader is referred to Chapter 1 of [23] for more information about the Galois theory of linear difference equations.

The group  $G$  can be reformulated as the stabilizer of some ideal in a  $\sigma$ -ring, which we describe below. Let  $Y$  denote an  $n \times n$  matrix  $(y_{i,j})$ , where the  $y_{i,j}$  are indeterminates. Sometimes, in brief, we also consider  $Y$  as a set of indeterminates. By setting  $\sigma(Y) = AY$ , one can extend  $\sigma$  from  $k$  to  $k[Y, 1/\det(Y)]$  so that it becomes a difference extension ring of  $k$ . The results in Section 1.1 of [23] imply that  $R$  is isomorphic to  $k[Y, 1/\det(Y)]/I$  for some maximal  $\sigma$ -ideal  $I$ . Define an action of  $\text{GL}_n(\overline{\mathbb{Q}})$  on  $k[Y, 1/\det(Y)]$  given by  $g \cdot Y = Yg$  for all  $g \in \text{GL}_n(\overline{\mathbb{Q}})$ . Suppose that  $J$  is an ideal of  $k[Y, 1/\det(Y)]$ . The *stabilizer* of  $J$ , denoted by  $\text{stab}(J)$ , is defined as

$$\text{stab}(J) = \{g \in \text{GL}_n(\overline{\mathbb{Q}}) \mid P(Yg) \in J, \forall P \in J\},$$

which is an algebraic subgroup of  $\text{GL}_n(\overline{\mathbb{Q}})$ . Set

$$I_F = \{P \in k[Y, 1/\det(Y)] \mid P(F) = 0\}.$$

Then  $I_F$  is a maximal  $\sigma$ -ideal and  $G = \text{stab}(I_F)$ . By the uniqueness of the Picard-Vessiot extension ring of  $k$  for (1), one sees that for any maximal  $\sigma$ -ideal  $I$  of  $k[Y, 1/\det(Y)]$ , there is  $g \in \text{GL}_n(\overline{\mathbb{Q}})$  such that  $g \cdot I = I_F$ . From this, one can readily verify the stabilizers of maximal  $\sigma$ -ideals in  $k[Y, 1/\det(Y)]$  are conjugated. In other words, as linear algebraic groups, these stabilizers are isomorphic. Therefore we shall also call the stabilizer of a maximal  $\sigma$ -ideal of  $k[Y, 1/\det(Y)]$  the Galois group of (1) over  $k$ . Using the Gröbner base method, one can obtain the defining equations of  $\text{stab}(I)$  easily once a Gröbner basis of  $I$  is known. Therefore,

the above definition indicates that finding a maximal  $\sigma$ -ideal of  $k[Y, 1/\det(Y)]$  will suffice to determine the Galois group. We shall give in this paper an algorithm that computes a maximal  $\sigma$ -ideal of  $k[Y, 1/\det(Y)]$ .

The rest of the paper is organized as follows. In Section 2, we introduce some basic results that provide the theoretical background of our algorithm. Meanwhile, we introduce some basic definitions such as proto-groups, proto-maximal  $\sigma$ -ideals and so on. In Section 3, we show how to compute a proto-maximal  $\sigma$ -ideal. In Section 4, we describe a method to extend a proto-maximal  $\sigma$ -ideal to a maximal  $\sigma^\delta$ -ideal so that one can easily obtain a maximal  $\sigma$ -ideal by taking the intersection of ideals. In Section 5, the methods developed in the previous sections are summarized as an algorithm, and an example is presented to illustrate the algorithm. In Appendix A, we describe a method to find coefficient bounds for generators of a proto-maximal  $\sigma$ -ideal. In Appendix B, an algorithm for computing  $\sigma^\delta$ -hypergeometric elements in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  is developed, where  $I_{\text{irr}}$  is a prime  $\sigma^\delta$ -ideal.

## 2 Some basic results

In this section, we shall introduce some basic results about proto-groups,  $k$ -torsors and several related problems whose algorithmic solutions will be needed in our algorithm.

### 2.1 Proto-groups

As in the differential case, bounds on algebraic subgroups of  $\text{GL}_n(\overline{\mathbb{Q}})$  play a central role in the main algorithm presented in this paper. Let  $H$  be an algebraic subgroup of  $\text{GL}_n(\overline{\mathbb{Q}})$ . For the ease of notation, we shall use  $H(k)$  (resp.  $H(\bar{k})$ ) to denote  $k$ -points (resp.  $\bar{k}$ -points) of  $H$ . We shall say  $H$  is bounded by a positive integer  $d$  if there is a set  $\mathbb{S} \subseteq \overline{\mathbb{Q}}[Y]$  such that  $H$  is the set of zeroes of  $\mathbb{S}$  in  $\text{GL}_n(\overline{\mathbb{Q}})$  and elements of  $\mathbb{S}$  are of degree not greater than  $d$ . In brief,  $H_u$  stands for the algebraic subgroup of  $H$  generated by unipotent elements and  $H^\circ$  denotes the identity component of  $H$ .

**Definition 2.1** *Let  $G, H$  be two algebraic subgroups of  $\text{GL}_n(\overline{\mathbb{Q}})$ .  $H$  is said to be a proto-group of  $G$  if they satisfy the following condition*

$$H_u \leq G^\circ \leq G \leq H.$$

*In the case that  $G$  is the Galois group of (1) over  $k$ ,  $H$  is called a proto-Galois group of (1).*

**Remark 2.2** *Suppose that  $H$  is a proto-group of  $G$  and  $\bar{H}$  is an algebraic subgroup satisfying  $G \leq \bar{H} \leq H$ . Since  $\bar{H}_u \leq H_u$ , one sees that  $\bar{H}$  is also a proto-group of  $G$ .*

For the convenience, we introduce the following definition.

**Definition 2.3** *A  $\sigma$ -ideal  $I$  in  $k[Y, 1/\det(Y)]$  is called proto-maximal if  $\text{stab}(I)$  is a proto-Galois group of (1).*

The key point of Hrushovski's algorithm is the following proposition, which is also the core of our algorithm.

**Proposition 2.4** (Corollary 3.7 of [11], Corollary B.15 of [7]) *One can find an integer  $\tilde{d}$  only depending on  $n$  such that for any algebraic subgroup  $G$  of  $\mathrm{GL}_n(\overline{\mathbb{Q}})$ , there is a proto-group of  $G$  bounded by  $\tilde{d}$ . Particularly, given linear differential equations, there exists a proto-Galois group of it bounded by the integer  $\tilde{d}$ .*

The integer  $\tilde{d}$  can be explicitly given as follows (see Corollary B.15 of [7] for details). Set

$$\kappa_1 = \max_i \left\{ \left( \binom{n^2 + (2n)^{3 \cdot 8^{n^2}}}{i} \right)^2 \right\}, \quad \kappa_2 = \kappa_1 (2n)^{3 \cdot 8^{n^2}} \binom{n^2 + (2n)^{3 \cdot 8^{n^2}}}{n^2} \quad (2)$$

and

$$\kappa_3 = \kappa_2 (\kappa_1^2 + 1) \max_i \left\{ \binom{\kappa_1^2 + 1}{i} \right\}, \quad I(n) = J \left( \max_i \left\{ \binom{n^2 + 1}{i} \right\} \right)$$

where  $J(m)$  is a Jordan bound, which is not greater than  $(\sqrt{8m} + 1)^{2m^2} - (\sqrt{8m} - 1)^{2m^2}$ . Then

$$\tilde{d} = (\kappa_3)^{I(n)-1}. \quad (3)$$

It is well-known in the theory of linear algebraic groups that any algebraic subgroup of a diagonalizable group  $D$  is the intersection of kernels of some characters of  $D$  (see Proposition in the page 103 of [10]). Given a connected algebraic group  $H$ , the following proposition describes algebraic subgroups that are the intersections of some characters of  $H$ .

**Proposition 2.5** *Suppose that  $H$  is a connected algebraic subgroup of  $\mathrm{GL}_n(\overline{\mathbb{Q}})$ . Then  $G$  is the intersection of kernels of some characters of  $H$  if and only if  $H$  is a proto-group of  $G$ .*

PROOF. Assume that  $H$  is a proto-group of  $G$ . Let  $\chi_1, \dots, \chi_\ell$  be generators of  $X(H)$ , the group of characters of  $H$ . Define a map  $\psi : H \rightarrow (\overline{\mathbb{Q}}^\times)^\ell$  given by  $\psi(h) = (\chi_1(h), \dots, \chi_\ell(h))$ , where  $\overline{\mathbb{Q}}^\times$  denotes the multiplicative group of  $\overline{\mathbb{Q}}$ . Then  $\psi(H)$  is a diagonalizable group and  $\psi(G)$  is one of its algebraic subgroups. Due to Proposition in the page 103 of [10],  $\psi(G)$  is the intersection of kernels of some characters of  $\psi(H)$ . Denote these characters by  $\bar{\chi}_1, \dots, \bar{\chi}_l$ . Notice that  $\psi$  induces a group homomorphism

$$\begin{aligned} \psi^* : X \left( (\overline{\mathbb{Q}}^\times)^\ell \right) &\rightarrow X(H) \\ \chi &\rightarrow \chi \circ \psi. \end{aligned}$$

We claim that  $G = \bigcap_{i=1}^l \ker(\psi^*(\bar{\chi}_i))$ . Obviously,  $G \subseteq \bigcap_{i=1}^l \ker(\psi^*(\bar{\chi}_i))$ . Suppose that  $h \in \bigcap_{i=1}^l \ker(\psi^*(\bar{\chi}_i))$ . Then  $\bar{\chi}_i(\psi(h)) = 1$  for all  $1 \leq i \leq l$ . This implies that  $\psi(h) \in \psi(G)$ . Lemma B.9 of [10] states that  $H_u = \ker(\psi)$ . Hence  $\ker(\psi) \subseteq G$  and then  $h \in G$ .

Conversely,  $G$  is the intersection of some characters of  $H$ . Then  $H_u = \ker(\psi) \subseteq G$ . Since  $H_u$  is connected,  $H_u \subseteq G^\circ$ . Thus  $H$  is a proto-group of  $G$ .  $\square$

The connection between proto-groups and  $\sigma$ -ideals in  $k[Y, 1/\det(Y)]$  is the geometric objects so called  $k$ -torsors, which are introduced in the next section.

## 2.2 $k$ -Torsors

We shall use  $\text{Zero}(J)$  to denote the set of zeroes of  $J$  in  $\text{GL}_n(\bar{k})$ , where  $J$  is a subset of  $k[Y, 1/\det(Y)]$ . Suppose that  $Z \subseteq \text{GL}_n(\bar{k})$  is a variety defined over  $k$ . We shall use  $I_k(Z)$  to denote the set of all polynomials in  $k[Y, 1/\det(Y)]$  that vanish on  $Z$ .

**Definition 2.6** (see Definition 3.13 of [22]) *Let  $Z \subseteq \text{GL}_n(\bar{k})$  be a variety defined over  $k$  and  $H$  an algebraic subgroup of  $\text{GL}_n(\bar{k})$  defined over  $k$ .  $Z$  is said to be a  $k$ -torsor for  $H$  if for any  $z_1, z_2 \in Z$ , there is a unique  $h \in H$  such that  $z_1 = z_2 h$ . A  $k$ -torsor  $Z$  for  $H$  is said to be trivial if  $Z \cap \text{GL}_n(k) \neq \emptyset$ , i.e.  $Z = BH$  for some  $B \in \text{GL}_n(k)$ .*

Let  $I$  be a maximal  $\sigma$ -ideal of  $k[Y, 1/\det(Y)]$ . Then one has that

**Proposition 2.7** (Proposition 1.20, page 15 of [23])  *$\text{Zero}(I)$  is a trivial  $k$ -torsor for  $\text{stab}(I)$ .*

Suppose that  $H$  is a connected algebraic subgroup of  $\text{GL}_n(\bar{k})$ , which is defined over  $\bar{\mathbb{Q}}$ , and  $Z$  is a trivial  $k$ -torsor for  $H$ . Then for any  $B \in Z \cap \text{GL}_n(k)$ , the map given by

$$\begin{aligned} k[Y, 1/\det(Y)]/I_k(H) &\rightarrow k[Y, 1/\det(Y)]/I_k(Z) \\ P(Y) &\rightarrow P(B^{-1}Y) \end{aligned} \quad (4)$$

is an isomorphism of  $k$ -algebras. A theorem of Rosenlicht ([14, 18, 21]) implies that invertible regular functions on  $Z$  are closely related to characters of  $H$ . This theorem states: let  $H$  be a connected linear algebraic group defined over an algebraically closed field  $\bar{k}$  and  $y$  be a regular function on  $H$  with  $1/y$  also a regular function, then  $y$  is a  $\bar{k}$  multiple of a character. Notice that characters of  $H$  can be viewed as elements in  $\bar{\mathbb{Q}}[Y, 1/\det(Y)]/I_{\bar{\mathbb{Q}}}(H)$ .

**Lemma 2.8** *Suppose that  $J$  is a prime  $\sigma$ -ideal of  $k[Y, 1/\det(Y)]$  and  $\text{Zero}(J)$  is a trivial  $k$ -torsor for  $H$ . Let  $B \in \text{Zero}(J) \cap \text{GL}_n(k)$ . If  $\chi$  is a character of  $H$ , then  $\chi(B^{-1}Y)$  is invertible in  $k[Y, 1/\det(Y)]/J$ . Conversely, if  $P$  is an invertible element in  $k[Y, 1/\det(Y)]/J$ , then  $P = r\chi(B^{-1}Y)$  for some  $r \in k$  and some character  $\chi$  of  $H$ .*

PROOF. We only need to prove the second assertion. Since  $\bar{\mathbb{Q}}$  is algebraically closed,  $H$  viewed as a linear algebraic group defined over  $\bar{k}$  is still connected. The map (4) implies that  $P(BY)$  is invertible in  $k[Y, 1/\det(Y)]/I_k(H)$ . Applying the above theorem of Rosenlicht to  $P(BY)$ , one has that  $P(BY) = r\chi$  for some  $r \in \bar{k}$  and some character  $\chi$ . Observe that  $k[Y, 1/\det(Y)]/J$  is a  $\sigma$ -extension ring of  $k$ . Due to Lemma 1.19 in the page 15 of [23],  $(k[Y, 1/\det(Y)]/J) \cap \bar{k} = k$ . Hence  $(k[Y, 1/\det(Y)]/I_k(H)) \cap \bar{k} = k$ . We then conclude that  $r \in k$  and  $P = r\chi(B^{-1}Y)$ .  $\square$

In Section 4, one will see that invertible elements of  $k[Y, 1/\det(Y)]/J$  are actually  $\sigma$ -hypergeometric over  $k$ . In the case that  $J$  is a proto-maximal  $\sigma$ -ideal, algebraic relations among these  $\sigma$ -hypergeometric elements will reveal the characters of  $H$  that determine the Galois group  $G$ .

### 2.3 Some related problems

In this paper, we shall need the algorithmic solutions of the following problems.

- (P1) Given an ideal in  $k[Y]$ , compute a Gröbner basis of it with respect to some monomial ordering. The reader is referred to Section 2.7 of [4] and Section 5.5 of [1] for the algorithms.
- (P2) Given an unmixed ideal in  $k[Y]$ , compute its radical and its associated primes. There are several methods for this problem, for instance the methods presented in [8], Section 4 of [6], Section 8.7 of [1], parts 36 and 42 of [19].
- (P3) Compute the Galois group of linear difference equations of diagonal form. Equivalently, given  $b_1, \dots, b_\ell \in k$ , compute a set of generators of the following  $\mathbb{Z}$ -module:

$$\left\{ (z_1, \dots, z_\ell) \in \mathbb{Z}^\ell \mid \exists f \in k \text{ s.t. } \prod_{i=1}^{\ell} b_i^{z_i} = \frac{\sigma(f)}{f} \right\}.$$

When  $k = \mathbb{Q}(x)$ , a method was described in Section 2.2 of [23]. Using the results in Section 3.2 of [5], one can adapt the method in [23] to solve the problem with  $k = \overline{\mathbb{Q}}(x)$ . This problem is the bottleneck in extending our algorithm to the equations over a larger basic field.

- (P4) Give linear difference equations with coefficients in  $k$ , compute all hypergeometric solutions. The reader is referred to ([3, 16]) for algorithms.

## 3 The computation of a proto-maximal $\sigma$ -ideal

Let  $F$  be a fundamental matrix of (1) and let  $d$  be a positive integer or  $\infty$ . Denote

$$I_{F,d} = \langle \{P(Y) \in k[Y]_{\leq d} \mid P(F) = 0\} \rangle, \quad (5)$$

where  $k[Y]_{\leq d}$  denotes the set of polynomials in  $k[Y]$  with degrees not greater than  $d$ , and  $\langle * \rangle$  denotes the ideal in  $k[Y, 1/\det(Y)]$  generated by  $*$ . When  $d = \infty$ ,  $I_{F,d}$  is equal to  $I_F$  that is defined in Introduction. One can readily verify that  $I_{F,d}$  is a  $\sigma$ -ideal and furthermore  $I_F$  is a maximal  $\sigma$ -ideal. The fact that  $k[Y, 1/\det(Y)]$  is a noetherian ring implies that for sufficiently large  $d$ ,  $I_{F,d}$  is a proto-maximal  $\sigma$ -ideal. Therefore to achieve a proto-maximal  $\sigma$ -ideal, one only needs to solve the following two problems: (a) Given an integer  $d$ , how to compute  $I_{F,d}$ ? (b) When is the integer  $d$  large enough such that  $I_{F,d}$  is proto-maximal?

### 3.1 The computation of $I_{F,d}$

In [12], Kauers and Zimmerman presented an algorithm for computing generators for the ideal of algebraic relations among solutions of linear difference equations with constant coefficients. Their algorithm relies on the fact that one can explicitly write down solutions of the equations of such type. Here, our task is different. We only compute the ideal generated by algebraic relations with bounded degree, while we are interested in linear difference equations with coefficients in  $k$ .

We first show that which fundamental matrix  $F$  we take in this section. Let  $\mathcal{S}_{\overline{\mathbb{Q}}}$  be the difference ring of germs at infinity of  $\overline{\mathbb{Q}}$  (see Example 1.3 in the page 4 of [23] for the definition). Let  $\rho$  be a nonnegative integer such that  $i$  is not a pole of entries of  $A$  and  $\det(A(i)) \neq 0$  if  $i \geq \rho$  and  $Z_\rho \in \mathrm{GL}_n(\overline{\mathbb{Q}})$ . Define an element of  $\mathrm{GL}_n(\mathcal{S}_{\overline{\mathbb{Q}}})$ , say  $\mathbf{Z} = (Z_0, Z_1, \dots)$ , as follows:  $Z_i = 0$  for  $0 \leq i \leq \rho - 1$  and  $Z_{i+1} = A(i)Z_i$  for  $i \geq \rho$ . Define a map

$$\psi : k[Y, 1/\det(Y)] \rightarrow \mathcal{S}_{\overline{\mathbb{Q}}}$$

as follows:

$$\text{for } f \in k, \psi(f) = (0, \dots, 0, f(i), f(i+1), \dots) \text{ and } \psi(Y) = \mathbf{Z}$$

where  $i$  is a nonnegative integer such that  $j$  is not a pole of  $f$  if  $j \geq i$ . Proposition 4.1 in the page 45 of [23] states that  $\psi$  induces an embedding of  $k[Y, 1/\det(Y)]/I$  into  $\mathcal{S}_{\overline{\mathbb{Q}}}$ , where  $I = \ker(\psi)$  that is a maximal  $\sigma$ -ideal. Let  $F$  be the image of  $Y$  in  $k[Y, 1/\det(Y)]/I$ . From this construction, we have that  $I_{F,d} = I_{\mathbf{Z},d}$ .

The results in Appendix A imply that one can compute an integer  $\ell$  such that  $I_{F,d}$  has a set of generators consisting of polynomials in  $\overline{\mathbb{Q}}[x][Y]$  whose degrees in  $x$  are not greater than  $\ell$ . Let  $N = \binom{d+n^2}{d} - 1$  and  $\mathbf{m}_0, \dots, \mathbf{m}_N$  be all elements in  $\mathbb{Z}_{\geq 0}^{n^2}$  with  $|\mathbf{m}_i| \leq d$ . Write  $P = \sum c_{j(\ell+1)+i} x^i Y^{\mathbf{m}_j}$  for  $P \in I_{F,d}$ , where  $Y^{\mathbf{m}_i} = \prod y_{j,l}^{m_{i,j,l}}$  with  $\mathbf{m}_i = (m_{i,j,l})$ . We can then reduce the original problem to the following problem: find a basis of the vector space

$$U = \left\{ (c_0, c_1, \dots, c_{(N+1)(\ell+1)-1}) \in \overline{\mathbb{Q}}^{(N+1)(\ell+1)} \mid \sum_{i=0}^{\ell} \sum_{j=0}^N c_{j(\ell+1)+i} x^i F^{\mathbf{m}_j} = 0 \right\}.$$

We are going to solve the latter problem. Observe that  $\sigma(x^i F^{\mathbf{m}_j})$  is a  $k$ -linear combination of the monomials  $F^{\mathbf{m}_0}, \dots, x^i F^{\mathbf{m}_j}, \dots, x^\ell F^{\mathbf{m}_N}$ . Hence there is a nonzero linear difference operator  $L$  in  $\overline{\mathbb{Q}}[x][\partial]$  such that  $L(x^i F^{\mathbf{m}_j}) = 0$  for all  $i$  with  $0 \leq i \leq \ell$  and  $0 \leq j \leq N$ . This operator  $L$  can be computed using the equation (1). Notice that at present, we do not know the ideal  $I$  and thus do not know  $F$ . Fortunately, one can easily compute the sequence solution  $\mathbf{Z}$ , which can be considered as a difference analogue of formal power series solutions of linear differential equations.

For the convenience, write (1) and  $L$  in the form of linear recurrence equations

$$Y_{m+1} = A(m)Y_m, m \geq \rho \tag{6}$$

and

$$L = a_l(m)y_{m+l} + a_{l-1}(m)y_{m+l-1} + \dots + a_0(m)y_m, m \geq \nu \tag{7}$$

where  $\rho$  is a positive integer such that  $i$  is not a pole of entries of  $A(x)$  and  $\det(A(i)) \neq 0$  for all  $i \geq \rho$ , and  $\nu$  is an integer greater than integer roots of  $a_l(x)a_0(x) = 0$ . One easily sees that

**Lemma 3.1** *Assume that  $\{s_\nu, s_{\nu+1}, \dots\}$  is a solution of (7). If there is a nonnegative integer  $j$  such that  $s_{\nu+j} = \dots = s_{\nu+l-1+j} = 0$ , then  $s_i = 0$  for all  $i \geq \nu$ .*



Let  $\kappa$  be an integer greater than  $\rho$  and  $\nu$ . Notice that the sequence  $\{Z_\rho, Z_{\rho+1}, \dots\}$  is a solution of (6) and for all  $0 \leq i \leq \ell$  and  $0 \leq j \leq N$ , the sequence  $\{\kappa^i Z_\kappa^{\mathbf{m}_j}, (\kappa+1)^i Z_{\kappa+1}^{\mathbf{m}_j}, \dots\}$  is a solution of (7). Set

$$P_{\mathbf{c}}(x, Y) = \sum_{i=0}^{\ell} \sum_{j=0}^N c_{j(\ell+1)+i} x^i Y^{\mathbf{m}_j}, \text{ where } \mathbf{c} = (c_0, \dots, c_{(N+1)(\ell+1)-1}) \in \overline{\mathbb{Q}}^{(N+1)(\ell+1)}.$$

Then the sequence  $\{P_{\mathbf{c}}(\kappa, Z_\kappa), (P_{\mathbf{c}}(\kappa+1, Z_{\kappa+1}), \dots\}$  is also a solution of (7).

**Proposition 3.2**  $\mathbf{c} \in U$  if and only if  $P_{\mathbf{c}}(i, Z_i) = 0$  for all  $\kappa \leq i \leq \kappa + l - 1$ .

PROOF. Assume that  $\mathbf{c} \in U$ . Then  $P_{\mathbf{c}}(x, F) = 0$  and thus  $\psi(P_{\mathbf{c}}(x, F)) = 0$ . In other words, there is a positive integer  $j$  such that  $P_{\mathbf{c}}(i, Z_i) = 0$  for all  $i \geq j$ . Lemma 3.1 implies that  $P_{\mathbf{c}}(i, Z_i) = 0$  for all  $\kappa \leq i \leq \kappa + l - 1$ . Conversely, suppose that  $P_{\mathbf{c}}(i, Z_i) = 0$  for all  $\kappa \leq i \leq \kappa + l - 1$ . By Lemma 3.1 again,  $P_{\mathbf{c}}(i, Z_i) = 0$  for all  $i \geq \kappa$ . This implies that  $\psi(P_{\mathbf{c}}(x, F)) = 0$ . Equivalently,  $P_{\mathbf{c}}(x, F) = 0$ . Hence  $\mathbf{c} \in U$ .  $\square$

The conditions  $P_{\mathbf{c}}(i, Z_i) = 0$  for all  $\kappa \leq i \leq \kappa + l - 1$  induce a linear system for  $\mathbf{c}$ . Solving this system, we obtain a basis of  $U$ .

**Algorithm 3.3** Compute a basis of  $I_{F,d}$ .

- (i) Using the results in Appendix A, compute an integer  $\ell$  such that  $I_{F,d}$  has generators consisting of polynomials in  $\mathbb{Q}[x][Y]$  whose degrees in  $x$  are not greater than  $\ell$ .
- (ii) Construct a nonzero operator  $L$  in  $\overline{\mathbb{Q}}[x][\partial]$  that annihilates  $x^i F^{\mathbf{m}_j}$  for all  $0 \leq i \leq \ell$  and  $0 \leq j \leq N$ , where  $\mathbf{m}_0, \dots, \mathbf{m}_N$  are all elements in  $\mathbb{Z}_{\geq 0}^{n^2}$  satisfying  $|\mathbf{m}_i| \leq d$ .
- (iii) Let  $\kappa$  be an integer that is greater than both  $\rho$  and all integer roots of the leading and trailing coefficients of  $L$ .
- (iv) Compute  $Z_\kappa, Z_{\kappa+1}, \dots, Z_{\kappa+l-1}$ , where  $l = \text{ord}(L)$ . Set

$$P_{\mathbf{c}}(x, Y) = \sum_{i=0}^{\ell} \sum_{j=0}^N c_{j(\ell+1)+i} x^i Y^{\mathbf{m}_j}, \mathbf{c} = (c_0, \dots, c_{(N+1)(\ell+1)-1}).$$

Putting  $P_{\mathbf{c}}(\kappa, Z_\kappa) = \dots = P_{\mathbf{c}}(\kappa + l - 1, Z_{\kappa+l-1}) = 0$ , we obtain a linear system  $\mathcal{L}$  in  $c_0, c_1, \dots, c_{(N+1)(\ell+1)-1}$ .

- (v) Solve  $\mathcal{L}$  and return  $\left\{ P_{\bar{\mathbf{c}}}(x, Y) \mid \bar{\mathbf{c}} \in \text{Zero}(\mathcal{L}) \cap \overline{\mathbb{Q}}^{(N+1)(\ell+1)} \right\}$ .

**Example 3.4** Consider the Fibonacci numbers  $F(n)$ . It satisfies that

$$\begin{pmatrix} F(n+1) \\ F(n+2) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} F(n) \\ F(n+1) \end{pmatrix}.$$

Let

$$\mathbf{Z} = \left( I_2, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2, \dots \right).$$



We are going to calculate  $I_{\mathbf{Z},2}$ . Using the results in Appendix A, one sees that there are generators of  $I_{\mathbf{Z},2}$  whose degrees in  $x$  are zero. Let  $\mathbf{m}_0, \dots, \mathbf{m}_{14}$  be all vectors in  $\mathbb{Z}_{\geq 0}^4$  satisfying  $|\mathbf{m}_i| \leq 2$ . Let

$$L = \partial^6 - 4\partial^5 + 2\partial^4 + 6\partial^3 - 4\partial^2 - 2\partial + 1.$$

Then  $L$  annihilates  $\mathbf{Z}^{\mathbf{m}_i}$  for all  $0 \leq i \leq 14$ . Computing the first 6 terms of  $\mathbf{Z}$ , denoted by  $Z_i$  for  $i = 0, \dots, 5$ . Set  $\mathbf{c} = (c_0, c_1, \dots, c_{14})$  and let  $P_{\mathbf{c}}(x, Y)$  be defined as in the step (d). Then

$$P_{\mathbf{c}}(x, Z_0) = c_0 + c_1 + c_4 + c_5 + c_8 + c_{14},$$

$$P_{\mathbf{c}}(x, Z_1) = c_0 + c_2 + c_3 + c_4 + c_9 + c_{10} + c_{11} + c_{12} + c_{13} + c_{14},$$

$$P_{\mathbf{c}}(x, Z_2) = c_0 + c_1 + c_2 + c_3 + 2c_4 + c_5 + c_6 + c_7 + 2c_8 + c_9 + c_{10} + 2c_{11} + c_{12} + 2c_{13} + 4c_{14},$$

$$P_{\mathbf{c}}(x, Z_3) = c_0 + c_1 + 2c_2 + 2c_3 + 3c_4 + \dots + 4c_{12} + 6c_{13} + 9c_{14},$$

$$P_{\mathbf{c}}(x, Z_4) = c_0 + 2c_1 + 3c_2 + 3c_3 + 5c_4 + \dots + 9c_{12} + 15c_{13} + 25c_{14},$$

$$P_{\mathbf{c}}(x, Z_5) = c_0 + 3c_1 + 5c_2 + 5c_3 + 8c_4 + \dots + 25c_{12} + 40c_{13} + 64c_{14}.$$

Solving the linear system  $\{P_{\mathbf{c}}(x, Z_i) | i = 0, \dots, 5\}$ , one has that

$$c_0 = 0, c_1 = -c_4, c_2 = -c_4 - c_3, c_5 = -c_8 - c_{14},$$

$$c_6 = -c_8 - 2c_{14} - c_7 - c_{11} - c_{13}, c_9 = -c_{14} - c_{10} - c_{11} - c_{12} - c_{13}.$$

From this, one sees that  $I_{\mathbf{Z},2}$  is generated by

$$y_{2,1} - y_{1,2}, y_{2,2} - y_{1,2} - y_{1,1}.$$

### 3.2 When is $I_{F,d}$ proto-maximal?

Let  $\tilde{d}$  be as in (3). In this section, we shall show that  $I_{F,\tilde{d}}$  is proto-maximal. Before proving this, we first describe some properties of  $I_{F,d}$ . Note that  $I_{F,d}$  is contained in a maximal  $\sigma$ -ideal  $I$ . Proposition 1.20 in the page 15 of ([23]) states that  $\text{Zero}(I)$  is a trivial  $k$ -torsor for  $\text{stab}(I)$ . We show that a similar property holds for  $I_{F,d}$ , i.e.  $\text{Zero}(I_{F,d})$  is a trivial  $k$ -torsor for  $\text{stab}(I_{F,d})$ . As  $\text{Zero}(I)$  is a trivial  $k$ -torsor for  $\text{stab}(I)$ ,  $\text{Zero}(I) \cap \text{GL}_n(k) \neq \emptyset$ . Therefore  $\text{Zero}(I_{F,d}) \cap \text{GL}_n(k) \neq \emptyset$ . For short, we denote by  $H_{F,d}$  the stabilizer of  $I_{F,d}$ .

**Lemma 3.5** *Let  $B$  be an element of  $\text{Zero}(I_{F,d}) \cap \text{GL}_n(k)$ . Then*

$$I_{F,d} = \left\langle \left\{ Q(B^{-1}Y) \mid Q \in I_{\overline{\mathbb{Q}}}(H_{F,d}) \cap \overline{\mathbb{Q}}[Y]_{\leq d} \right\} \right\rangle.$$

PROOF. Denote by  $J_B$  the right-hand side. Suppose that  $P$  is an element of  $k[Y]_{\leq d}$  with  $P(F) = 0$ . Then for each  $h \in H_{F,d}$ ,  $P(Yh) \in I_{F,d}$  and therefore  $P(Bh) = 0$ . Write

$$P(BY) = \sum_{i=1}^l c_i P_i(Y)$$

where  $P_i(Y) \in \overline{\mathbb{Q}}[Y]$  and  $c_1, \dots, c_l$  are linearly independent over  $\overline{\mathbb{Q}}$ . Obviously, for all  $i$  with  $1 \leq i \leq l$ , the degree of  $P_i(Y)$  is not greater than  $d$  and  $P_i(h) = 0$  for all  $h \in H_{F,d}$ . In other words,  $P_i(Y) \in I_{\overline{\mathbb{Q}}}(H_{F,d}) \cap \overline{\mathbb{Q}}[Y]_{\leq d}$  for all  $i = 1, \dots, l$ . Hence  $P \in J_B$  and then  $I_{F,d} \subseteq J_B$ .

Notice that  $I_F$  is a maximal  $\sigma$ -ideal that contains  $I_{F,d}$ . Let  $G = \text{stab}(I_F)$ . Observe that the action of  $\text{GL}_n(\overline{\mathbb{Q}})$  on  $k[Y]$  preserves the degrees of polynomials. From the definition of  $I_{F,d}$ , one sees that  $G \subseteq H_{F,d}$ . Due to Proposition 2.7,  $\text{Zero}(I_F) = \bar{B}G(\bar{k})$  for any  $\bar{B} \in \text{Zero}(I_F) \cap \text{GL}_n(k)$ . This implies that  $\text{Zero}(I_F) \subseteq \text{Zero}(J_{\bar{B}})$  and thus  $J_{\bar{B}} \subseteq I_F$ . As  $F$  is a zero of  $I_F$ , it is also a zero of  $J_{\bar{B}}$ . This together with the fact that  $J_{\bar{B}}$  is generated by polynomials in  $k[Y]_{\leq d}$  implies that  $J_{\bar{B}} \subseteq I_{F,d}$ . On the other hand, the previous result shows that  $I_{F,d} \subseteq J_{\bar{B}}$ . Consequently,  $I_{F,d} = J_{\bar{B}}$ . It remains to prove that  $J_B = J_{\bar{B}}$ .

We first have that  $J_{\bar{B}} \subseteq J_B$ . Define a  $k$ -automorphism  $\phi$  of  $k[Y]$  as follows:

$$\phi(P(Y)) = P(\bar{B}B^{-1}Y).$$

Then  $\phi(J_{\bar{B}}) = J_B$ , which implies that  $J_B \subseteq \phi(J_B) \subseteq \phi^2(J_B) \subseteq \dots$ . Due to the noetherian property of  $k[Y, 1/\det(Y)]$ ,  $J_B = \phi(J_B)$ . In the sequel,  $J_B = J_{\bar{B}}$ .  $\square$

The above lemma has the following corollaries.

**Corollary 3.6** *Let  $B$  be an element of  $\text{Zero}(I_{F,d}) \cap \text{GL}_n(k)$ . Then*

$$\text{Zero}(I_{F,d}) = BH_{F,d}(\bar{k})$$

*i.e.  $\text{Zero}(I_{F,d})$  is a trivial  $k$ -torsor for  $H_{F,d}$ .*

**Corollary 3.7** *Let  $I_{\text{irr}}$  be an associated prime of  $I_{F,d}$ . Then  $\text{stab}(I_{\text{irr}}) = H_{F,d}^\circ$ . Moreover  $\text{Zero}(I_{\text{irr}})$  is a trivial  $k$ -torsor for  $H_{F,d}^\circ$ .*

PROOF. Let  $B$  be an element of  $\text{Zero}(I_{\text{irr}}) \cap \text{GL}_n(k)$ . By Corollary 3.6,

$$\text{Zero}(I_{\text{irr}}) \cap \text{GL}_n(\bar{k}) = BH_i(\bar{k})$$

where  $H_i$  is an irreducible component of  $H_{F,d}$ . Since  $B \in \text{Zero}(I_{\text{irr}})$ ,  $H_i = H_{F,d}^\circ$ . Thus  $\text{Zero}(I_{\text{irr}})$  is a trivial  $k$ -torsor for  $H_{F,d}^\circ$ . For each  $g \in \text{GL}_n(\bar{k})$ , one can define an isomorphism  $\phi_g$  of  $\text{GL}_n(\bar{k})$  given by  $\phi_g(Z) = Zg$ . As  $I_{\text{irr}}$  is prime, one can verify that  $h \in \text{stab}(I_{\text{irr}})$  if and only if  $\phi_h(BH_{F,d}^\circ(\bar{k})) = BH_{F,d}^\circ(\bar{k})$ . On the other hand, for  $h \in \text{GL}_n(\overline{\mathbb{Q}})$ ,  $\phi_h(BH_{F,d}^\circ(\bar{k})) = BH_{F,d}^\circ(\bar{k})$  if and only if  $h \in H_{F,d}^\circ$ . Therefore  $\text{stab}(I_{\text{irr}}) = H_{F,d}^\circ$ .  $\square$

**Lemma 3.8** *Suppose that  $\bar{F}$  is a fundamental matrix of (1). If  $\bar{F}$  is a zero of  $I_{F,d}$ , then*

$$I_{F,d} = I_{\bar{F},d}.$$

PROOF. From the assumption, one has that  $I_{F,d} \subseteq I_{\bar{F},d}$ . Observe that  $F = \bar{F}h$  for some  $h \in \text{GL}_n(\overline{\mathbb{Q}})$ . The definition of  $I_{F,d}$  implies that  $\phi_h(I_{F,d}) = I_{\bar{F},d}$ , where the homomorphism  $\phi_h$  is given by  $\phi_h(Y) = Yh$ . The successive applications of  $\phi_h$  to  $I_{F,d} \subseteq I_{\bar{F},d}$  induce that

$$I_{\bar{F},d} \subseteq \phi_h(I_{\bar{F},d}) \subseteq \dots \subseteq \phi_h^i(I_{\bar{F},d}) \subseteq \dots$$

The noetherian property of the ring  $k[Y, 1/\det(Y)]$  implies that  $I_{\bar{F},d} = \phi_h(I_{\bar{F},d})$ . Therefore  $\phi_h(I_{F,d}) = \phi_h(I_{\bar{F},d})$ , i.e.  $I_{F,d} = I_{\bar{F},d}$ .  $\square$

**Proposition 3.9**  $\text{stab}(I_{F,\tilde{d}})$  is a proto-group of  $\text{stab}(I)$ , where  $I$  is any maximal  $\sigma$ -ideal containing  $I_{F,\tilde{d}}$ . In other words,  $I_{F,\tilde{d}}$  is proto-maximal.

PROOF. Let  $G = \text{stab}(I)$  and  $H$  be an algebraic subgroup of  $\text{GL}_n(\overline{\mathbb{Q}})$  that is bounded by  $\tilde{d}$  and is a proto-group of  $G$ . Such  $H$  exists by Proposition 2.4. Observe that there is a fundamental matrix  $\bar{F}$  such that  $I = I_{\bar{F}}$ . Since  $I_{F,\tilde{d}} \subseteq I$ , we have that  $I_{\bar{F},\tilde{d}} = I_{F,\tilde{d}}$  due to Lemma 3.8. Let  $B$  be an element of  $\text{Zero}(I) \cap \text{GL}_n(k)$  and let

$$J = \left\{ Q(B^{-1}Y) \mid Q \in I_{\overline{\mathbb{Q}}}(H) \cap \overline{\mathbb{Q}}[Y]_{\leq \tilde{d}} \right\}.$$

Since  $H$  is bounded by  $\tilde{d}$ ,  $\text{Zero}(J) = BH(\bar{k})$ . By Proposition 2.7,  $\text{Zero}(I) = BG(\bar{k})$ . Therefore  $J \subseteq I$ , because  $I$  is radical and  $H$  is a proto-group of  $G$ . Note that  $\bar{F}$  is a zero of  $I$ . One then has that  $\bar{F}$  is a zero of  $J$ . This implies that

$$J \subseteq I_{\bar{F},\tilde{d}} = I_{F,\tilde{d}} \subseteq I.$$

The first inclusion holds because  $J$  is generated by a set of polynomials in  $k[Y]_{\leq \tilde{d}}$ . Lemma 3.5 then implies that

$$G \leq H_{F,\tilde{d}} \leq H.$$

Then the proposition follows from Remark 2.2.  $\square$

**Example 3.10** Consider

$$\sigma \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ x & 0 & 0 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}. \quad (8)$$

Using the method developed in Section 3.1, we can compute a  $\sigma$ -ideal

$$I_{\mathbf{Z},2} = \langle y_{1,1}y_{1,2}, y_{1,1}y_{1,3}, y_{1,1}y_{2,1}, y_{1,1}y_{2,3}, y_{1,1}y_{3,1}, y_{1,1}y_{3,2}, y_{1,2}y_{1,3}, y_{1,2}y_{2,1}, y_{1,2}y_{2,2}, y_{1,2}y_{3,2}, y_{1,2}y_{3,3}, \\ y_{1,3}y_{2,2}, y_{1,3}y_{2,3}, y_{1,3}y_{3,1}, y_{1,3}y_{3,3}, y_{2,1}y_{2,2}, y_{2,1}y_{2,3}, y_{2,1}y_{3,1}, y_{2,1}y_{3,3}, y_{2,2}y_{2,3}, y_{2,2}y_{3,1}, y_{2,2}y_{3,2}, \\ y_{2,3}y_{3,2}, y_{2,3}y_{3,3}, y_{3,1}y_{3,2}, y_{3,1}y_{3,3}, y_{3,2}y_{3,3} \rangle.$$

Furthermore, one has that

$$\text{stab}(I_{\mathbf{Z},2}) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \alpha\beta\gamma \neq 0 \right\} \cup \left\{ \begin{pmatrix} 0 & \alpha & 0 \\ 0 & 0 & \beta \\ \gamma & 0 & 0 \end{pmatrix} \middle| \alpha\beta\gamma \neq 0 \right\} \cup \left\{ \begin{pmatrix} 0 & 0 & \alpha \\ \beta & 0 & 0 \\ 0 & \gamma & 0 \end{pmatrix} \middle| \alpha\beta\gamma \neq 0 \right\}.$$

Since all elements in  $\text{stab}(I_{\mathbf{Z},2})$  is semi-simple,  $\text{stab}(I_{\mathbf{Z},2})$  is a proto-Galois group of (1) over  $k$ , i.e.  $I_{\mathbf{Z},2}$  is a proto-maximal  $\sigma$ -ideal.

## 4 The computation of a maximal $\sigma^\delta$ -ideal

The results in the previous section enable us to calculate a proto-maximal  $\sigma$ -ideal. Suppose that we have obtained a proto-maximal  $\sigma$ -ideal, say  $I_{F,\tilde{d}}$ . Let  $I_{\text{irr}}$  be an associated prime of  $I_{F,\tilde{d}}$ . It can be obtained by the algorithmic solutions of the problem (P1). Since  $I_{F,\tilde{d}}$  is a

$\sigma$ -ideal,  $I_{\text{irr}}$  is a  $\sigma^\delta$ -ideal for some positive integer  $\delta$ . In the following, we will enlarge  $I_{\text{irr}}$  to obtain a maximal  $\sigma^\delta$ -ideal. By Corollary 3.7, one sees that for any  $B \in \text{Zero}(I_{\text{irr}}) \cap \text{GL}_n(k)$ ,

$$\text{Zero}(I_{\text{irr}}) = BH_{F,\tilde{d}}^\circ(\bar{k}) \text{ and } \text{stab}(I_{\text{irr}}) = H_{F,\tilde{d}}^\circ. \quad (9)$$

Let  $I_\delta$  be a maximal  $\sigma^\delta$ -ideal that contains  $I_{\text{irr}}$ . Proposition 2.7 implies that  $\text{Zero}(I_\delta)$  is a trivial  $k$ -torsor for  $\text{stab}(I_\delta)$ , i.e.  $\text{Zero}(I_\delta) = BG_\delta(\bar{k})$  where  $B \in \text{Zero}(I_\delta) \cap \text{GL}_n(k)$ . Then the equality (9) induces that  $\text{stab}(I_\delta) \subseteq H_{F,\tilde{d}}^\circ$ . We shall show that  $H_{F,\tilde{d}}^\circ$  is a proto-group of  $\text{stab}(I_\delta)$ .

**Lemma 4.1** *Let  $\tilde{I}$  be a maximal  $\sigma^\delta$ -ideal and  $I = \tilde{I} \cap \sigma(\tilde{I}) \cap \cdots \cap \sigma^{\delta-1}(\tilde{I})$ . Then*

- (a)  $I$  is a maximal  $\sigma$ -ideal.
- (b)  $[\text{stab}(I) : \text{stab}(\tilde{I})] \leq \delta$ .

PROOF. (a). Suppose that  $\tilde{I}$  is a maximal  $\sigma$ -ideal. Let  $J$  be a maximal  $\sigma^\delta$ -ideal containing  $\tilde{I}$ . Then  $\tilde{I} \subseteq \cap_{i=0}^{\delta-1} \sigma^i(J)$ . On the other hand,  $\cap_{i=0}^{\delta-1} \sigma^i(J)$  is a  $\sigma$ -ideal and thus it is equal to  $\tilde{I}$ . For any  $g \in \text{GL}_n(\overline{\mathbb{Q}})$ , one can define a  $\sigma$ -isomorphism  $\phi_g$  of  $k[Y, 1/\det(Y)]$  given by  $\phi_g(Y) = Yg$ . From the uniqueness of the Picard Vessiot extensions, one can easily see that there is  $g \in \text{GL}_n(\overline{\mathbb{Q}})$  such that  $\phi_g(J) = \tilde{I}$ . This implies that  $\phi_g(\tilde{I}) = I$ . Hence  $I$  is a maximal  $\sigma$ -ideal.

(b). Let  $G = \text{stab}(I)$  and  $\tilde{G} = \text{stab}(\tilde{I})$ . Let  $B$  be an element of  $\text{Zero}(\tilde{I}) \cap \text{GL}_n(k)$ . Due to Proposition 2.7, one has that

$$\text{Zero}(I) = BG(\bar{k}) \text{ and } \text{Zero}(\tilde{I}) = B\tilde{G}(\bar{k}). \quad (10)$$

Meanwhile, all  $\sigma^i(\tilde{I})$  are maximal  $\sigma^\delta$ -ideals. Hence there are  $g_1, \dots, g_{\delta-1} \in \text{GL}_n(\overline{\mathbb{Q}})$  such that  $\phi_{g_i}(\sigma^i(\tilde{I})) = \tilde{I}$ . This implies that

$$\text{Zero}(\sigma^i(\tilde{I})) = B\tilde{G}(\bar{k})g_i, \quad i = 0, 1, \dots, \delta - 1. \quad (11)$$

The equalities (10) and (11) imply that  $G = \cup_{i=0}^{\delta-1} \tilde{G}g_i$ . In the sequel,  $[G : \tilde{G}] \leq \delta$ .  $\square$

Let  $I = I_\delta \cap \sigma(I_\delta) \cap \cdots \cap \sigma^{\delta-1}(I_\delta)$ . Then  $I_{F,\tilde{d}} \subseteq I$ . The above lemma together with Proposition 3.9 induces that  $H_{F,\tilde{d}}$  is a proto-group of  $\text{stab}(I)$ , i.e.

$$\left(H_{F,\tilde{d}}\right)_u \leq (\text{stab}(I))^\circ \leq \text{stab}(I) \leq H_{F,\tilde{d}}.$$

Observe that  $\left(H_{F,\tilde{d}}\right)_u = \left(H_{F,\tilde{d}}^\circ\right)_u$ . Due to the above lemma again,  $(\text{stab}(I))^\circ = (\text{stab}(I_\delta))^\circ$ . Thus

$$\left(H_{F,\tilde{d}}^\circ\right)_u \leq (\text{stab}(I_\delta))^\circ \leq \text{stab}(I_\delta) \leq H_{F,\tilde{d}}^\circ$$

i.e.  $H_{F,\tilde{d}}^\circ$  is a proto-group of  $\text{stab}(I_\delta)$ . Proposition 2.5 implies that  $\text{stab}(I_\delta)$  is the intersection of kernels of some characters of  $H_{F,\tilde{d}}^\circ$ . This will enable us to construct  $I_\delta$ . Suppose that  $\bar{\chi}_1, \dots, \bar{\chi}_l$  are characters of  $H_{F,\tilde{d}}^\circ$  satisfying

$$\ker(\bar{\chi}_1) \cap \cdots \cap \ker(\bar{\chi}_l) = \text{stab}(I_\delta).$$

Then we have the following lemma.

**Lemma 4.2** *Let  $B$  be an element of  $\text{Zero}(I_\delta) \cap \text{GL}_n(k)$  and*

$$\mathbb{S} = I_{\text{irr}} \cup \{\bar{\chi}_i(B^{-1}Y) - 1 \mid i = 1, \dots, l\}.$$

*Then  $\text{Zero}(I_\delta) = \text{Zero}(\mathbb{S})$ .*

PROOF. Let  $G_\delta = \text{stab}(I_\delta)$ . It suffices to show that  $\text{Zero}(\mathbb{S}) = BG_\delta(\bar{k})$ . Observe that  $B \in \text{Zero}(I_{\text{irr}}) \cap \text{GL}_n(k)$ , which implies that  $\text{Zero}(I_{\text{irr}}) = BH_{F,\bar{d}}^\circ(\bar{k})$ . Suppose that  $Z \in BG_\delta(\bar{k})$ . As  $G_\delta$  is the intersection of kernels of the characters  $\bar{\chi}_1, \dots, \bar{\chi}_l$ , one sees that  $Z \in \text{Zero}(\mathbb{S})$ . Conversely, assume that  $Z \in \text{Zero}(\mathbb{S})$ . Then  $Z \in \text{Zero}(I_{\text{irr}})$  and thus  $Z = Bh$  for some  $h \in H_{F,\bar{d}}^\circ(\bar{k})$ . Meanwhile for each  $i = 1, \dots, l$ ,

$$\bar{\chi}_i(B^{-1}Z) = \bar{\chi}_i(h) = 1.$$

This implies that  $h \in G_\delta(\bar{k})$ . Therefore  $\text{Zero}(\mathbb{S}) = BG_\delta(\bar{k})$ .  $\square$

Proposition 2.7 states that invertible elements of  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  are  $k$  multiples of characters of  $H_{F,\bar{d}}^\circ$ . Precisely, let  $P$  be an invertible element of  $k[Y, 1/\det(Y)]/I_{\text{irr}}$ , then  $P = r\chi(B^{-1}Y)$  for some  $r \in k$  and some character  $\chi$  of  $H_{F,\bar{d}}^\circ$ . By the above lemma, to compute  $I_\delta$ , it suffices to find invertible elements of  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  that take constant values on  $\text{Zero}(I_\delta)$ . In the following, we first show that invertible elements of  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  are actually  $\sigma^\delta$ -hypergeometric over  $k$  and then prove that algebraic relations among  $\sigma^\delta$ -hypergeometric elements take constant values on  $\text{Zero}(I_\delta)$  and enable us to find  $I_\delta$ . We start with a definition.

**Definition 4.3** *A nonzero element  $P$  of  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  is said to be  $\sigma^\delta$ -hypergeometric over  $k$  if  $P$  is invertible in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  and  $\sigma^\delta(P) = rP$  for some  $r \in k$ .*

Let  $P_1, P_2$  be two  $\sigma^\delta$ -hypergeometric elements over  $k$  of  $k[Y, 1/\det(Y)]/I_{\text{irr}}$ . We say  $P_1$  and  $P_2$  are *similar* if there is  $r \in k$  such that  $P_1 = rP_2$ .

**Proposition 4.4** *Let  $B$  be an element of  $\text{Zero}(I_{\text{irr}}) \cap \text{GL}_n(k)$  and  $\chi$  a character of  $H_{F,\bar{d}}^\circ$  that is represented by an element of  $\overline{\mathbb{Q}}[Y, 1/\det(Y)]$ . Then  $\chi(B^{-1}Y)$  is a  $\sigma^\delta$ -hypergeometric element over  $k$  of  $k[Y, 1/\det(Y)]/I_{\text{irr}}$ . Furthermore, if  $\chi_1$  and  $\chi_2$  are two distinct characters, then  $\chi_1(B^{-1}Y)$  and  $\chi_2(B^{-1}Y)$  are not similar.*

PROOF. Obviously,  $\chi(B^{-1}Y)$  is invertible in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$ . We first claim that

$$\sigma^\delta(B^{-1})A_\delta B \in H_{F,\bar{d}}^\circ(k).$$

For any  $Q \in I_{\overline{\mathbb{Q}}}(H_{F,\bar{d}}^\circ)$ , by (9),  $Q(B^{-1}Y) \in I_{\text{irr}}$ . As  $I_{\text{irr}}$  is a  $\sigma^\delta$ -ideal, one has that  $Q(\sigma^\delta(B^{-1})A_\delta Y) \in I_{\text{irr}}$ . Since  $B \in \text{Zero}(I_{\text{irr}})$ ,  $Q(\sigma^\delta(B^{-1})A_\delta B) = 0$ . This proves the claim. Now for any  $h \in H_{F,\bar{d}}^\circ(\bar{k})$ ,

$$\chi(\sigma^\delta(B^{-1})A_\delta Bh) - \chi(\sigma^\delta(B^{-1})A_\delta B)\chi(B^{-1}Bh) = 0.$$

This implies that

$$\chi(\sigma^\delta(B^{-1})A_\delta Y) - \chi(\sigma^\delta(B^{-1})A_\delta B)\chi(B^{-1}Y) \in I_{\text{irr}}.$$

In other words,

$$\sigma^\delta(\chi(B^{-1}Y)) - \chi(\sigma^\delta(B^{-1})A_\delta B)\chi(B^{-1}Y) \in I_{\text{irr}},$$

i.e.  $\chi(B^{-1}Y)$  is a  $\sigma^\delta$ -hypergeometric element over  $k$  of  $k[Y, 1/\det(Y)]/I_{\text{irr}}$ . This proves the first assertion.

Now assume that  $\chi_1(B^{-1}Y) - r\chi_2(B^{-1}Y) \in I_{\text{irr}}$  for some  $r \in k$ . Then for any  $h \in H_{F,\tilde{d}}^\circ$ ,

$$\chi_1(h) = \chi_1(B^{-1}Bh) = r\chi_2(B^{-1}Bh) = r\chi_2(h).$$

Particularly, putting  $h = I_n$ , one then has that  $r = 1$ . Thus  $\chi_1 = \chi_2$ , a contradiction.  $\square$

Let  $\kappa_2$  be as in (2). Proposition B.17 of [7] states that  $X(H_{F,\tilde{d}}^\circ)$  has generators that are represented by polynomials in  $\overline{\mathbb{Q}}[Y]_{\leq \kappa_2}$ . Denote

$$\mathcal{H} = \left\{ P \in k[Y]_{\leq \kappa_2} \left| \begin{array}{l} P \text{ is } \sigma^\delta\text{-hypergeometric over } k \text{ in } k[Y, 1/\det(Y)]/I_{\text{irr}}, \\ P - rQ \notin I_{\text{irr}}, \forall r \in k, \forall Q \in \mathcal{H} \setminus \{P\} \end{array} \right. \right\}$$

and

$$\mathcal{X} = \left\{ P \in \overline{\mathbb{Q}}[Y]_{\leq \kappa_2} \left| \begin{array}{l} P \in X(H_{F,\tilde{d}}^\circ), \\ P - Q \notin I_k(H_{F,\tilde{d}}^\circ), \forall Q \in \mathcal{X} \setminus \{P\} \end{array} \right. \right\}.$$

Then  $\mathcal{X}$  is a set of generators of  $X(H_{F,\tilde{d}}^\circ)$ . Furthermore, we have that

**Corollary 4.5** *There is a bijective map between  $\mathcal{H}$  and  $\mathcal{X}$ .*

PROOF. Let  $B \in \text{Zero}(I_{\text{irr}}) \cap \text{GL}_n(k)$ . We define a map  $\tau$  from  $\mathcal{H}$  to  $X(H_{F,\tilde{d}}^\circ)$  as follows:  $\tau(P) = \chi$  where  $\chi \in X(H_{F,\tilde{d}}^\circ)$  satisfies  $P - r\chi(B^{-1}Y) \in I_{\text{irr}}$  for some  $r \in k$ . By Proposition 2.7, for each  $P \in \mathcal{H}$ , there is a character  $\chi$  such that  $\tau(P) = \chi$ , and such character is unique by Proposition 4.4. Hence  $\tau$  is well-defined. From the definition of  $\mathcal{H}$ , one sees that  $\tau$  is injective. We shall prove that  $\tau(\mathcal{H}) = \mathcal{X}$ . As the map defined in (4) is an isomorphism, one has that

$$P(BY)/r - \chi(Y) \in I_k(H_{F,\tilde{d}}^\circ).$$

Hence  $\chi(Y)$  can be chosen to be a polynomial in  $\overline{\mathbb{Q}}[Y]_{\leq \kappa_2}$ . That is,  $\chi \in \mathcal{X}$ . Therefore  $\tau(\mathcal{H}) \subseteq \mathcal{X}$ . Finally, Proposition 4.4 implies that  $\tau(\mathcal{H}) = \mathcal{X}$ .  $\square$

Algorithm B.1 in Appendix B enables us to compute  $\mathcal{H}$ . Suppose that  $\mathcal{H} = \{P_1, \dots, P_\nu\}$ . Let  $b_j$  be the certifications of  $P_j$ , i.e.  $\sigma^\delta(P_j) - b_j P_j \in I_{\text{irr}}$  for all  $1 \leq j \leq \nu$ . Set

$$\mathcal{Z} = \left\{ (m_1, \dots, m_\nu) \in \mathbb{Z}^\nu \left| \exists f \in k^\times, \text{ s.t. } \prod_{j=1}^\nu b_j^{m_j} = \frac{\sigma^\delta(f)}{f} \right. \right\}.$$

$\mathcal{Z}$  is a finitely generated  $\mathbb{Z}$ -module. The solution of the problem (P4) allows us to compute a set of generators of  $\mathcal{Z}$ . Assume that  $\mathbf{m}_1, \dots, \mathbf{m}_\mu$  are generators of  $\mathcal{Z}$  and further suppose that

$$\prod_{j=1}^{\nu} b_j^{m_{i,j}} = \frac{\sigma^\delta(f_i)}{f_i}$$

where  $f_i \in k$  and  $\mathbf{m}_i = (m_{i,1}, \dots, m_{i,\mu})$ . For each  $i = 1, \dots, \mu$ , write  $\mathbf{m}_i = \mathbf{m}_i^+ - \mathbf{m}_i^-$ , where  $\mathbf{m}_i^+, \mathbf{m}_i^-$  are in  $\mathbb{Z}_{\geq 0}^\nu$  and  $\mathbf{m}_i^+ (\mathbf{m}_i^-)^T = 0$ . Denote by  $\mathbf{P}$  the vector  $(P_1, \dots, P_\mu)$  and  $\mathbf{P}^{\mathbf{m}} = \prod_{j=1}^{\nu} P_j^{m_j}$  where  $\mathbf{m} = (m_1, \dots, m_\nu)$ . Let

$$\mathcal{P} = \left\langle I_{\text{irr}} \cup \left\{ \mathbf{P}^{\mathbf{m}_i^+} - f_i \mathbf{P}^{\mathbf{m}_i^-} \mid i = 1, \dots, \mu \right\} \right\rangle$$

It is easy to verify that  $\mathcal{P}$  is a  $\sigma^\delta$ -ideal. Let  $I_\delta$  be a maximal  $\sigma^\delta$ -ideal containing  $\mathcal{P}$ . Then

**Proposition 4.6**  $\text{Zero}(\mathcal{P}) = \text{Zero}(I_\delta)$ , i.e.  $I_\delta = \sqrt{\mathcal{P}}$ .

PROOF. Let  $B$  be an element of  $\text{Zero}(I_\delta) \cap \text{GL}_n(k)$  and  $G_\delta = \text{stab}(I_\delta)$ . Then due to Proposition 2.7,

$$\text{Zero}(I_\delta) = BG_\delta(\bar{k}).$$

The discussion after Lemma 4.1 states that  $H_{F,\bar{d}}^\circ$  is a proto-group of  $G_\delta$ . By Proposition 2.5,  $G_\delta$  is the intersection of kernels of some characters of  $H_{F,\bar{d}}^\circ$ . Let  $\Lambda$  be the set of these characters. Observe that  $\mathcal{X}$  is a set of generators of  $X(H_{F,\bar{d}}^\circ)$ . Suppose that  $\bar{\chi} \in \Lambda$ . Then

$$\bar{\chi} = \prod_{i=1}^{\nu} \tau(P_i)^{\alpha_i}, \quad (12)$$

where  $\alpha_i \in \mathbb{Z}$  and  $\tau$  is defined as in Corollary 4.5. By Corollary 4.5, for each  $i = 1, \dots, \nu$ , there is  $r_i \in k$  such that

$$\tau(P_i)(B^{-1}Y) - r_i P_i \in I_{\text{irr}}. \quad (13)$$

Lemma 4.2 implies that  $\bar{\chi}(B^{-1}Y) - 1 \in I_\delta$ . Denote by  $\bar{Y}$  the image of  $Y$  in  $k[Y, 1/\det(Y)]/I_\delta$ . Then  $\bar{\chi}(B^{-1}\bar{Y}) - 1 = 0$ . This together with (12) and (13) induces that

$$\prod_{i=1}^{\nu} r_i^{\alpha_i} P_i^{\alpha_i}(\bar{Y}) - 1 = 0. \quad (14)$$

Applying  $\sigma^\delta$  to (14), one has that

$$\prod_{i=1}^{\nu} \sigma^\delta(r_i^{\alpha_i}) b_i^{\alpha_i} P_i^{\alpha_i}(\bar{Y}) - 1 = 0. \quad (15)$$

Combining (14) and (15), one has that

$$\prod_{i=1}^{\nu} b_i^{\alpha_i} = \prod_{i=1}^{\nu} \frac{\sigma^\delta(r_i^{-\alpha_i})}{r_i^{-\alpha_i}}.$$



Set  $\alpha = (\alpha_1, \dots, \alpha_\nu) \in \mathbb{Z}^\nu$ . Then  $\alpha \in \mathcal{Z}$ . So there are integers  $z_1, \dots, z_\mu$  such that  $\alpha = z_1 \mathbf{m}_1 + \dots + z_\mu \mathbf{m}_\mu$ .

Let  $Z$  be an element of  $\text{Zero}(\mathcal{P})$ . Then one has that  $\mathbf{P}^{\mathbf{m}_i}(Z) = f_i$  for all  $1 \leq i \leq \mu$ , because  $\mathbf{P}^{\mathbf{m}_i^-}(Z) \neq 0$ . By (12) and (13) again,

$$\begin{aligned} \bar{\chi}(B^{-1}Z) - 1 &= \prod_{i=1}^{\nu} \tau(P_i)^{\alpha_i}(B^{-1}Z) - 1 = \mathbf{P}^\alpha(Z) \prod_{i=1}^{\nu} r_i^{\alpha_i} - 1 \\ &= \prod_{i=1}^{\mu} \mathbf{P}^{z_i \mathbf{m}_i}(Z) \prod_{i=1}^{\nu} r_i^{\alpha_i} - 1 = \prod_{i=1}^{\mu} f_i^{z_i} \prod_{i=1}^{\nu} r_i^{\alpha_i} - 1. \end{aligned}$$

This implies that the polynomial  $\bar{\chi}(B^{-1}X) - 1$  takes a constant value on  $\text{Zero}(\mathcal{P})$ . Particularly, putting  $Z = B$ , one has that  $\bar{\chi}(B^{-1}B) - 1 = \prod_{i=1}^{\mu} f_i^{z_i} \prod_{i=1}^{\nu} r_i^{\alpha_i} - 1 = 0$ . In the sequel,  $\bar{\chi}(B^{-1}Z) - 1 = 0$  for all  $Z \in \text{Zero}(\mathcal{P})$ . Therefore

$$\text{Zero}(\mathcal{P}) \subseteq \text{Zero}(I_{\text{irr}} \cup \{\bar{\chi}(B^{-1}Y) - 1 \mid \bar{\chi} \in \Lambda\}).$$

The former set contains  $\text{Zero}(I_\delta)$  and the latter one is equal to  $\text{Zero}(I_\delta)$  by Lemma 4.2. Consequently,  $\text{Zero}(\mathcal{P}) = \text{Zero}(I_\delta)$ .  $\square$

Suppose that  $\mathcal{P}$  has been calculated. One can then compute  $\sqrt{\mathcal{P}}$  by the methods developed in ([6], Section 8.7 of [1]) and  $I = \sqrt{\mathcal{P}} \cap \sigma(\sqrt{\mathcal{P}}) \cap \dots \cap \sigma^{\delta-1}(\sqrt{\mathcal{P}})$  by the algorithm presented in (Section 6.3, page 260 of [1]). Then the ideal  $I$  is a maximal  $\sigma$ -ideal by Lemma 4.1.

**Example 4.7** (*Example 3.10 continued*) We have the following irreducible decomposition:

$$\begin{aligned} I_{\mathbf{Z},2} &= \langle y_{1,1}, y_{1,2}, y_{2,2}, y_{2,3}, y_{3,1}, y_{3,3} \rangle \cap \langle y_{1,1}, y_{1,3}, y_{2,1}, y_{2,2}, y_{3,2}, y_{3,3} \rangle \\ &\quad \cap \langle y_{1,2}, y_{1,3}, y_{2,1}, y_{2,3}, y_{3,1}, y_{3,2} \rangle. \end{aligned}$$

Set  $I_{\text{irr}} = \langle y_{1,1}, y_{1,2}, y_{2,2}, y_{2,3}, y_{3,1}, y_{3,3} \rangle$ . Then one can easily verify that  $I_{\text{irr}}$  is a  $\sigma^3$ -ideal and

$$\text{stab}(I_{\text{irr}}) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \alpha\beta\gamma \neq 0 \right\}.$$

The group of characters of  $X(\text{stab}(I_{\text{irr}}))$  is generated by  $y_{1,1}, y_{2,2}, y_{3,3}$ . Thus we only need to compute  $\sigma^3$ -hypergeometric elements in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  which are represented by linear polynomials in  $k[Y]$ . By Algorithm B.1, we have that  $y_{1,3}, y_{2,1}, y_{3,2}$  are  $\sigma^3$ -hypermetric elements of  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  and further they are not similar in pair. Precisely,

$$\sigma^3(y_{1,3}) = (x+2)y_{1,3}, \quad \sigma^3(y_{2,1}) = xy_{2,1}, \quad \sigma^3(y_{3,2}) = (x+1)y_{3,2}.$$

An easy calculation implies that the only element  $(m_1, m_2, m_3)$  in  $\mathbb{Z}^3$  such that

$$x^{m_1}(x+1)^{m_2}(x+2)^{m_3} = \sigma^3(f)/f$$

for some  $f \in k$  is  $(0, 0, 0)$ . This implies that  $I_{\text{irr}}$  is a maximal  $\sigma^3$ -ideal.

## 5 The algorithm and an example

We are now ready to present the algorithm for computing the Galois group  $\text{stab}(I)$ , where  $I$  is a maximal  $\sigma$ -ideal of  $k[Y, 1/\det(Y)]$ .

**Algorithm 5.1** *Input: linear difference equations of the form (1).*

*Output: the Galois group of (1) over  $k$ .*

- (i) Compute a proto-maximal ideal  $I_{F,\tilde{d}}$  by Algorithm 3.3.
- (ii) Using algorithms for the problem (P2), compute an associated prime of  $I_{F,\tilde{d}}$ , denoted by  $I_{\text{irr}}$ . Compute a positive integer  $\delta$  such that  $I_{\text{irr}}$  is a  $\sigma^\delta$ -ideal.
- (iii) By Algorithm B.1, compute  $\sigma^\delta$ -hypergeometric elements in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  that are represented by polynomials in  $k[Y]_{\leq \kappa_2}$ , and are not similar in pair. Denote them by  $P_1, \dots, P_\nu$ .
- (iv) Let  $b_i$  be the certificates of  $P_i$ , i.e.  $\sigma^\delta(P_i) - b_i P_i \in I_{\text{irr}}$  where  $b_i \in k$  and  $i = 1, \dots, \nu$ . Using the method for the problem (P3), compute a set of generators of the following  $\mathbb{Z}$ -module

$$\mathcal{Z} = \left\{ (z_1, \dots, z_\nu) \in \mathbb{Z}^\nu \mid \exists f \in k^\times, \text{ s.t. } \prod_{i=1}^\nu b_i^{z_i} = \frac{\sigma^\delta(f)}{f} \right\}.$$

Denote those generators by  $\mathbf{m}_1, \dots, \mathbf{m}_\mu$ .

- (v) Set  $\mathbf{P} = (P_1, \dots, P_\nu)$  and find  $f_i$ , the element in  $k$  satisfying  $\mathbf{P}^{\mathbf{m}_i} = \sigma^\delta(f_i)/f_i$  where  $i = 1, \dots, \mu$ . Set

$$\mathcal{P} = I_{\text{irr}} \cup \left\{ \mathbf{P}^{\mathbf{m}_i^+} - f_i \mathbf{P}^{\mathbf{m}_i^-} \mid i = 1, \dots, \mu \right\},$$

where  $\mathbf{m}_i^+, \mathbf{m}_i^-$  are elements in  $\mathbb{Z}_{\geq 0}^\nu$  satisfying  $\mathbf{m}_i^+ - \mathbf{m}_i^- = \mathbf{m}_i$  and  $\mathbf{m}_i^+ (\mathbf{m}_i^-)^T = 0$ .

- (vi) By the algorithms for the problem (P1) and the algorithm presented in (Section 6.3, page 260 of [1]), compute  $\sqrt{\mathcal{P}}$  and

$$I = \sqrt{\mathcal{P}} \cap \sigma(\sqrt{\mathcal{P}}) \cap \dots \cap \sigma^{\delta-1}(\sqrt{\mathcal{P}}).$$

- (vii) Return  $\text{stab}(I)$ .

The correctness of the algorithm comes from the results presented in the previous sections.

**Remark 5.2** *One may suspect that the complexity of the algorithm would be very high, since the integers  $\tilde{d}$  and  $\kappa_2$  given in (2) and (3) are quite large. These integers guarantee the terminate of the algorithm. However, as shown in Examples 3.10 and 4.7, these integers may be much larger than those required in practice.*

In the following, we give an example to illustrate the algorithm.

**Example 5.3** Consider the following linear difference equations

$$\sigma \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ x & 0 & 0 \\ 0 & 0 & \frac{1}{x} \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}. \quad (16)$$

- (i) Using the method developed in Section 3.1, we compute an ideal  $\tilde{I}$  generated by polynomials in  $I_{F,2} \cap \overline{\mathbb{Q}}[Y]$ :

$$\tilde{I} = \langle y_{3,2}, y_{3,1}, y_{2,3}, y_{2,1}y_{2,2}, y_{1,3}, y_{1,2}y_{2,2}, y_{1,1}y_{2,1}, y_{1,1}y_{1,2} \rangle.$$

$\tilde{I}$  is a  $\sigma$ -ideal and

$$\text{stab}(\tilde{I}) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \alpha\beta\gamma \neq 0 \right\} \cup \left\{ \begin{pmatrix} 0 & \alpha & 0 \\ \beta & 0 & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \alpha\beta\gamma \neq 0 \right\}.$$

As all elements in  $\text{stab}(\tilde{I})$  are semi-simple,  $\text{stab}(\tilde{I})$  is a proto-maximal  $\sigma$ -ideal and thus  $\tilde{I}$  is a proto-maximal  $\sigma$ -ideal.

- (ii)  $\tilde{I}$  is radical and one can compute its irreducible decomposition as follows:

$$\tilde{I} = \langle y_{1,1}, y_{1,3}, y_{2,2}, y_{2,3}, y_{3,1}, y_{3,2} \rangle \cap \langle y_{1,2}, y_{1,3}, y_{2,1}, y_{2,3}, y_{3,1}, y_{3,2} \rangle.$$

Set  $I_{\text{irr}} = \langle y_{1,1}, y_{1,3}, y_{2,2}, y_{2,3}, y_{3,1}, y_{3,2} \rangle$ . Then  $I_{\text{irr}}$  is a  $\sigma^2$ -ideal and

$$\text{stab}(I_{\text{irr}}) = \{ \text{diag}(\alpha, \beta, \gamma) \mid \alpha\beta\gamma \neq 0 \}.$$

- (iii) Observe that the group of characters of  $\text{stab}(I_{\text{irr}})$  is generated by linear polynomials. Using Algorithm B.1, we can find that  $\sigma^2$ -hypergeometric elements of  $k[Y, 1/\det(Y)]/\text{irr}$  that are represented by linear polynomials in  $k[Y]$  are  $y_{1,2}, y_{2,1}, y_{3,3}$ . Precisely,

$$\sigma^2(y_{1,2}) = xy_{1,2}, \quad \sigma^2(y_{2,1}) = (x+1)y_{2,1}, \quad \sigma^2(y_{3,3}) = \frac{1}{x(x+1)}y_{3,3}.$$

- (iv) Set

$$\mathcal{Z} = \left\{ (z_1, z_2, z_3) \in \mathbb{Z}^3 \mid \exists f \in k^\times, \text{ s.t. } x^{z_1}(x+1)^{z_2} \left( \frac{1}{x(x+1)} \right)^{z_3} = \frac{\sigma^2(f)}{f} \right\}.$$

One sees that  $\mathcal{Z}$  is generated by  $(1, 1, 1)$ .

- (v) Let  $\mathcal{P} = \langle I_{\text{irr}} \cup \{y_{1,2}y_{2,1}y_{3,3} - 1\} \rangle$ . One has that  $\mathcal{P}$  is a radical ideal and thus is a maximal  $\sigma^2$ -ideal.

- (vi) Compute  $I = \mathcal{P} \cap \sigma(\mathcal{P})$ . One has that

$$I = \langle y_{3,2}, y_{3,1}, y_{2,3}, y_{2,2}y_{2,1}, y_{1,3}, y_{2,2}y_{1,2}, y_{1,2}y_{2,1}^2y_{3,3} - y_{2,1}, y_{1,2}^2y_{2,1}y_{3,3} - y_{1,2}, y_{1,2}y_{2,1}y_{3,3} + y_{1,1}y_{2,2}y_{3,3} - 1, y_{1,1}y_{2,1}, y_{1,1}y_{1,2} \rangle.$$

- (vii) Using the Gröbner base computation, we have that

$$\text{stab}(I) = \left\{ \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \alpha\beta\gamma = 1 \right\} \cup \left\{ \begin{pmatrix} 0 & \alpha & 0 \\ \beta & 0 & 0 \\ 0 & 0 & \gamma \end{pmatrix} \middle| \alpha\beta\gamma = 1 \right\}.$$

## A Coefficient bounds for generators of $I_{F,d}$

Note that  $I_{F,d}$  is generated by

$$\mathbb{S} = \{P(Y) \in k[Y]_{\leq d} \mid P(F) = 0\},$$

which is a  $k$ -vector space of finite dimension. We are going to find coefficient bounds for  $\mathbb{S}$ . Precisely, we shall find an integer  $\ell$  such that there is a basis of  $\mathbb{S}$  satisfying that coefficients of elements in this basis are of degree  $\leq \ell$ . Let  $N = \binom{d+n^2}{d}$  and  $M_1, \dots, M_N$  be the monomials in entries of  $F$  with degrees not greater than  $d$ . Observe that for a basis of  $\mathbb{S}$ , it suffices to find a basis of the following vector space

$$\left\{ (a_1, \dots, a_N) \in k^N \mid \sum_{i=1}^N a_i M_i = 0 \right\}.$$

Furthermore, one sees that  $(M_1, \dots, M_N)^T$  is a solution of linear difference equations, which can be constructed from (1). Hence our original problem can be reduced to the following.

**Problem A.1** Assume that  $\mathbf{v} = (v_1, \dots, v_n)^T$  is a nonzero solution of (1), where the  $v_i$  are in some Picard-Vessiot extension ring of  $k$ . Set

$$W = \{(a_1, a_2, \dots, a_n) \in k^n \mid a_1 v_1 + \dots + a_n v_n = 0\}.$$

Find an integer  $\ell$  depending on  $n$  and  $A$ , such that  $W$  has a basis consisting of vectors whose entries are of degree not greater than  $\ell$ .

Without loss of generality, we may assume that  $v_1, \dots, v_r$  are linearly independent over  $k$  and

$$v_{r+i} = c_{i,1} v_1 + \dots + c_{i,r} v_r, \quad i = 1, \dots, n-r.$$

For all  $i$  with  $1 \leq i \leq n-r$ , denote  $\mathbf{c}_i = (c_{i,1}, \dots, c_{i,2}, \dots, c_{i,n})$  where  $c_{i,r+i} = -1$  and  $c_{i,r+j} = 0$  for  $1 \leq j \leq n-r$  and  $j \neq i$ . Then  $\{\mathbf{c}_1, \dots, \mathbf{c}_{n-r}\}$  is a basis of  $W$ . Actually, for any  $\mathbf{a} = (a_1, \dots, a_n) \in W$ , we have that  $\mathbf{a} = -(a_{r+1} \mathbf{c}_1 + \dots + a_n \mathbf{c}_{n-r})$ . In the following, we are going to find a bound for  $\deg(c_{i,j})$ , where  $i = 1, \dots, n-r, j = 1, \dots, r$ . Let  $V$  be the solution space of (1) and

$$\tilde{V} = \{\mathbf{w} \in V \mid \mathbf{c}_i \mathbf{w}^T = 0, \quad \forall i = 1, \dots, n-r\}.$$

Then  $\tilde{V}$  is a  $\overline{\mathbb{Q}}$ -vector space of finite dimension. Moreover, we have

**Lemma A.2**  $\dim(\tilde{V}) = r$ .

PROOF. Clearly,  $\mathbf{v} \in \tilde{V}$ . Suppose that  $\{\mathbf{v}_1, \dots, \mathbf{v}_\mu\}$  is a basis of the vector space over  $\overline{\mathbb{Q}}$  spanned by the orbit of  $\mathbf{v}$  under the action of  $\text{Gal}(K/k)$ , the Galois group of (1), where  $K$  is the ring of fractions of the Picard Vessiot extension of  $k$  for (1). Then  $\mathbf{v}_i \in V$  for all  $i$  with  $1 \leq i \leq \mu$ . In the sequel,  $\dim(\tilde{V}) \geq \mu$ . In the following, we shall prove that  $\mu \geq r$ . Denote the matrix consisting of the first  $\mu$  rows of  $(\mathbf{v}_1, \dots, \mathbf{v}_\mu)$  by  $D$  and the remaining one by  $U$ . For any  $\phi \in \text{Gal}(K/k)$ , there is  $[\phi] \in \text{GL}_\mu(\overline{\mathbb{Q}})$  such that  $\phi(D) = D[\phi]$  and  $\phi(U) = U[\phi]$ .

Without loss of generality, we may assume that  $\det(D) \neq 0$ . As for any  $\phi \in \text{Gal}(K/k)$ ,  $\phi(\det(D)) = \det(D) \det([\phi])$ . One sees that  $\det(D)$  is invertible in  $K$  and therefore  $D$  is invertible. Now for any  $\phi \in \text{Gal}(K/k)$ ,

$$\phi(UD^{-1}) = U[\phi][\phi]^{-1}D^{-1} = UD^{-1}.$$

The Galois theory implies that  $C = UD^{-1} \in k^{(n-\mu) \times \mu}$ . Set  $\tilde{C} = (C, I_{n-\mu})$ . Then

$$\tilde{C} \begin{pmatrix} D \\ U \end{pmatrix} = 0.$$

Particularly,  $\tilde{C}\mathbf{v} = 0$ . This implies that  $\dim(W) = n - r \geq n - \mu$  and then  $\mu \geq r$ . So  $\dim(\tilde{V}) \geq r$ . On the other hand, one has that  $\dim(\tilde{V}) + n - r \leq n$  and then  $\dim(\tilde{V}) \leq r$ . Hence  $\dim(\tilde{V}) = r$ .  $\square$

Assume that  $\{\mathbf{v}_1 = \mathbf{v}, \mathbf{v}_2, \dots, \mathbf{v}_r\}$  is a basis of  $\tilde{V}$  and  $M$  is the  $n \times r$  matrix consisting of the vectors  $\mathbf{v}_1, \dots, \mathbf{v}_r$ . For  $1 \leq i_1 < \dots < i_r \leq n$ , denote the determinant of the sub-matrix consisting of the  $i_1$ -th,  $i_2$ -th,  $\dots$ ,  $i_r$ -th rows of  $M$  by  $d_{i_1, i_2, \dots, i_r}$ . Then an easy calculation implies that

$$d_{i_1, i_2, \dots, i_r} = b_{i_1, i_2, \dots, i_r} d_{1, 2, \dots, r}, \text{ where } b_{i_1, i_2, \dots, i_r} \in k.$$

In particular,  $b_{1, 2, \dots, j-1, j+1, \dots, r, r+i} = (-1)^{r-j} c_{i, j}$ . Let  $\mathbf{b} = (b_{1, 2, \dots, r}, \dots, b_{n-r+1, n-r+2, \dots, n})^T$ . On the other hand, one can construct from  $A$  an invertible matrix  $\tilde{A}_r$  with entries in  $k$  such that  $\mathbf{b}d_{1, 2, \dots, r}$  is a solution of  $\sigma(Y) = \tilde{A}_r Y$ . Notice that the matrix  $\tilde{A}_r$  only depends on  $A$  and  $r$ . Moreover, one can easily verify that  $d_{1, 2, \dots, r}$  is hypergeometric over  $k$ . This implies that  $\mathbf{b}d_{1, 2, \dots, r}$  is a hypergeometric solution. By means of cyclic vector, the system of the form (1) can be reduced into a scale linear difference equation. Then algorithms developed in ([3, 16]) allow us to find all hypergeometric solutions of  $\sigma(Y) = \tilde{A}_r Y$  are of the form  $\mathbf{w}h$  where  $h$  is hypergeometric over  $k$  and  $\mathbf{w}$  is a vector whose entries are elements in  $k$  with degree not greater than  $\ell/2$ . Particularly,  $\mathbf{b}d_{1, 2, \dots, r} = \bar{\mathbf{w}}\bar{h}$  where  $\bar{\mathbf{w}} = (\bar{w}_1, \dots, \bar{w}_n) \in k^n$  satisfying  $\deg(\bar{w}_i) \leq \ell/2$  and  $\bar{h}$  is hypergeometric over  $k$ . Observe that  $b_{1, 2, \dots, r} = 1$ . Then one has that  $\mathbf{b} = \bar{\mathbf{w}}/\bar{w}_1$ . Hence entries of  $\mathbf{b}$  are of degree  $\leq \ell$ , i.e.  $\deg(c_{i, j}) \leq \ell$ .

In the case that we do not know the dimension of  $\tilde{V}$ , we can take  $r = 1, 2, \dots, n$  and construct the corresponding systems  $\sigma(Y) = \tilde{A}_1 Y, \dots, \sigma(Y) = \tilde{A}_n Y$  respectively. Compute all hypergeometric solutions of these systems and let  $\ell/2$  be an integer such that these hypergeometric solutions are of the form  $\mathbf{w}h$  where  $h$  is hypergeometric over  $k$  and  $\mathbf{w}$  is a vector whose entries are rational functions in  $x$  with degrees not greater than  $\ell/2$ . Then we have that  $\deg(c_{i, j}) \leq \ell$ . This solves Problem A.1.

## B $\sigma^\delta$ -Hypergeometric elements

We shall describe a method to compute  $\sigma^\delta$ -hypergeometric elements in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$ . In fact, we are not going to calculate all  $\sigma^\delta$ -hypergeometric elements in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$ . Instead, we only find those  $\sigma^\delta$ -hypergeometric elements that are represented by polynomials in  $k[Y]$  with degrees not greater than  $d$  and furthermore that are not similar in pair. Assume

that  $\mathbf{m}_1, \dots, \mathbf{m}_\ell$  are polynomials in  $k[Y]_{\leq d}$  satisfying that  $\{\bar{\mathbf{m}}_1, \dots, \bar{\mathbf{m}}_\ell\}$  is a  $k$ -basis of  $k[Y]_{\leq d}/(I_{\text{irr}} \cap k[Y]_{\leq d})$ , where  $\bar{\mathbf{m}}_i$  is the image of  $\mathbf{m}_i$ . By the Gröbner base computation, one can find these  $\mathbf{m}_i$ . As  $\sigma^\delta$  preserves the degrees of elements of  $k[Y]$ , there is  $\tilde{A} \in \text{GL}_\ell(k)$  such that

$$\sigma^\delta((\bar{\mathbf{m}}_1, \bar{\mathbf{m}}_2, \dots, \bar{\mathbf{m}}_\ell)) = (\bar{\mathbf{m}}_1, \bar{\mathbf{m}}_2, \dots, \bar{\mathbf{m}}_\ell)\tilde{A}.$$

The invertible matrix  $\tilde{A}$  can be constructed from  $A$ . Now suppose that  $P = \sum c_i \mathbf{m}_i$  is a  $\sigma^\delta$ -hypergeometric element, where  $c_i \in k$ , i.e.  $\sigma^\delta(P) - rP \in I_{\text{irr}}$  for some  $r \in k$ . Then one can verify that  $c_1, \dots, c_\ell$  and  $r$  satisfying

$$\tilde{A}\sigma^\delta \begin{pmatrix} c_1 \\ \vdots \\ c_\ell \end{pmatrix} = r \begin{pmatrix} c_1 \\ \vdots \\ c_\ell \end{pmatrix}.$$

Let  $h$  be a  $\sigma^\delta$ -hypergeometric element satisfying  $\sigma^\delta(h) = rh$ . Then  $(c_1, \dots, c_\ell)^T h$  is a  $\sigma^\delta$ -hypergeometric solutions of the following linear difference equations

$$\sigma^\delta(Y) = \tilde{A}^{-1}Y. \quad (17)$$

Consequently, for those  $c_1, \dots, c_\ell$  and  $r$ , it suffices to find all  $\sigma^\delta$ -hypergeometric solutions of the above linear difference equations. The algorithms for computing all  $\sigma^\delta$ -hypergeometric solutions of (17) can be found at ([3, 16]). Particularly, one can find  $\sigma^\delta$ -hypergeometric solutions  $\mathbf{c}_1 h_1, \dots, \mathbf{c}_l h_l$  that are not similar in pair where  $h_1, \dots, h_l$  are  $\sigma^\delta$ -hypergeometric and  $\mathbf{c}_1, \dots, \mathbf{c}_l$  are vectors with entries in  $k$ . Here two vectors  $\mathbf{h}_1, \mathbf{h}_2$  are said to be similar if  $\mathbf{h}_1 = r\mathbf{h}_2$  for some  $r \in k^\times$ . Furthermore, if  $\mathbf{h}$  is a  $\sigma^\delta$ -hypergeometric solution of (17), then there is a unique  $j$  with  $1 \leq j \leq l$  satisfying  $\mathbf{h} = b\mathbf{c}_j h_j$  for some  $b \in k$ . Write  $\mathbf{c}_i = (c_{i,1}, \dots, c_{i,\ell})$  and set  $P_i = \sum_{j=1}^\ell c_{i,j} \mathbf{m}_j$ , where  $i = 1, 2, \dots, l$ . Then  $\sigma^\delta(P_i) - r_i P_i \in I_{\text{irr}}$  for some  $r_i \in k$ . It remains to select those  $P_i$  that are invertible in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$ . Note that  $P_i$  is invertible in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  if and only if  $\text{Zero}(P_i) \cap \text{Zero}(I_{\text{irr}}) = \emptyset$ . The latter condition can be detected by the Gröbner base computation. Precisely, it suffices to decide if 1 is in the ideal  $\langle I_{\text{irr}}, P_i \rangle$ . The previous results are summarized in the following algorithm.

**Algorithm B.1** Compute all  $\sigma^\delta$ -hypergeometric elements in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$  that are represented by polynomials in  $k[Y]_{\leq d}$  and are not similar in pair.

(a) Compute a Gröbner basis for  $I_{\text{irr}} \cap k[Y]$  and then find the monomials  $\mathbf{m}_1, \dots, \mathbf{m}_\ell$  in  $k[Y]_{\leq d}$  such that  $\{\bar{\mathbf{m}}_1, \dots, \bar{\mathbf{m}}_\ell\}$  is a  $k$ -basis of  $k[Y]_{\leq d}/(I_{\text{irr}} \cap k[Y]_{\leq d})$ , where  $\bar{\mathbf{m}}_i$  denotes the image of  $\mathbf{m}_i$  in  $k[Y, 1/\det(Y)]/I_{\text{irr}}$ .

(b) Construct an invertible matrix  $\tilde{A} \in \text{GL}_\ell(k)$  such that

$$\sigma^\delta((\bar{\mathbf{m}}_1, \bar{\mathbf{m}}_2, \dots, \bar{\mathbf{m}}_\ell)) = (\bar{\mathbf{m}}_1, \bar{\mathbf{m}}_2, \dots, \bar{\mathbf{m}}_\ell)\tilde{A}.$$

(c) Compute  $\sigma^\delta$ -hypergeometric elements

$$\sigma^\delta(Y) = \tilde{A}^{-1}Y$$

that are not similar in pair, say  $\mathbf{c}_1 h_1, \dots, \mathbf{c}_l h_l$ , where  $h_1, \dots, h_l$  are  $\sigma^\delta$ -hypergeometric and  $\mathbf{c}_1, \dots, \mathbf{c}_l$  are vectors with entries in  $k$ .

- (d) Write  $\mathbf{c}_i = (c_{i,1}, \dots, c_{i,\ell})$  and set  $P_i = \sum_{j=1}^{\ell} c_{i,j} \mathbf{m}_j$ , where  $i = 1, 2, \dots, l$ .
- (e) Decide whether  $k[Y, z] = \langle I_{\text{irr}} \cap k[Y], P_i, \det(Y)z - 1 \rangle$  by the Gröbner base computation. Return those  $P_i$  satisfying  $\langle I_{\text{irr}} \cap k[Y], P_i, \det(Y)z - 1 \rangle = k[Y, z]$ .

## References

- [1] Thomas Becker Volker Weispfenning, Gröbner Bases, Graduate Texts in Mathematics, Springer-Verlag, New York, Inc., 1993.
- [2] E. Compoint, Michael F. Singer, Computing Galois groups of completely reducible differential equations, J. Symbolic Comput. 28 (1999) 473-494.
- [3] T. Cluzeau, M. van Hoeij, Computing hypergeometric solutions of linear recurrence equations, AAECC, 17, 83-115, 2006.
- [4] D.A. Cox, J. Little, D. O'Shea, Ideals, Varieties, and Algorithms, Springer-Verlag, New York, 1996.
- [5] Harm Derksena, Emmanuel Jeandelb and Pascal Koiranb, Quantum automata and algebraic groups, J. Symbolic Comput., 39,357-371, 2005.
- [6] D. Eisenbud, C. Huneke, W. Vasconcelos, Direct methods for primary decomposition, Invent. math. 110 (1992) 207-235.
- [7] Ruyong Feng, Hrushovskis algorithm for computing the Galois group of a linear differential equation, Advances in Applied Mathematics, 65, 1-37, 2015.
- [8] P. Gianni, B. Trager and G. Zacharias, Gröbner bases and primary decomposition of polynomials ideals, J. Symbolic Comput. 6 (1988) 149-167.
- [9] Peter A. Hendriks, An Algorithm determining the difference Galois group of second order linear Difference equations, J. Symbolic Computation, 26, 445-461, 1998.
- [10] James E. Humphreys, Linear Algebraic Groups, Springer-Verlag New York, 1981.
- [11] Ehud Hrushovski, Computing the Galois group of a linear differential equation, Banach Center Publications, 58, 97-138, 2002.
- [12] Manuel Kauers and Burkhard Zimmermann, Computing the algebraic Relations of C-finite sequences and multisequences, J. Symbolic Comput., 43(11):787-803, 2008.
- [13] J.J. Kovacic, An algorithm for solving second order linear homogeneous differential equations, J. Symbolic Comput. 2,3-43,1986.
- [14] A. Magid, Finite generation of class groups of rings of invariants, Proc. Amer. Math. Soc., 60, 45-48, 1976.
- [15] A. Maier, A difference version of Noris theorem, Mathematische Annalen, 359(3-4),759-784,2014.



- [16] Mark Petkosevek, Hypergeometric solutions of linear recurrence equations with polynomial coefficients, J. Symbolic Comput., 14, 243-264, 1992.
- [17] Daniel Rettstadt, On the computation of the differential Galois group, Ph.D. thesis, RWTH Aachen University, 2014.
- [18] M. Rosenlicht, Toroidal algebraic groups, Proc. Amer. Math. Soc., 12, 984-988, 1961.
- [19] A. Seidenberg, Constructions in algebra, Trans. Amer. Math. Soc., 197, 273-313, 1974.
- [20] M.F. Singer, F. Ulmer, Galois groups of second and third order linear differential equations, J. Symbolic Comput. 16 (1993) 9-36.
- [21] M.F. Singer, Algebraic relations among solutions of linear differential equations, Trans. Amer. Math. Soc., 295, 753-763, 1986.
- [22] M.F. Singer, Algebraic and Algorithmic Aspects of Difference Equations, Lecture notes at CIMPA conference in Santa Marta Columbia, 2012.
- [23] Marius van der Put and Michael F. Singer, Galois Theory of Difference Equations, Lecture Notes in Mathematics 1666, Springer-Verlag, Berlin Heidelberg, 1997.